REMARKS/ARGUMENTS

By way of an Office Action mailed August 10, 2005, the Office Action rejects claims 1-21. Independent claims 1, 12, and 18 were rejected under 35 USC 102 as being anticipated by Ricahrd et al. Price, U.S. Patent No. 5,922,074. Dependent Claims 2-6, 13-16 and 19 were rejected under 35 U.S.C. § 103 as being obvious in light of Richard et al. in view of Donnelly ("Designing and LDAP Directory Tree", May 2000). Claims 8-11, 17, 20 and 21 were rejected under 35 U.S.C. § 103 as being obvious in light of Richard et al. in view of Donnelly, in further view of Knight et al. ("Cashing in on Caching", 1996).

Richard does not anticipate the independent claims as amended of the present invention since Richard does not claim or disclose the management and encryption using Public Keys.

Independent claims 1, 12 and 18, as amended, include the element of having computer readable instructions intercept an electronic message generated from the sender's e-mail account. Richard does not claim or disclose computer readable instructions that intercept a message generated from the sender's e-mail account. Richard, however, only receives the client identify, not an electronic message. (Richard, col 7, lines 507). Richard is only concerned with the identification of a client and not with providing public key information for encrypting a message using public keys from decentralized storage systems.

The Office Action also states that the first computer readable medium of the independent claims 1, 12 and 18 are anticipated by the server 42 of figures 1 and 2 of Richard. However, Richard does not claim or disclose the ability for the first set of

computer readable instructions to encrypt an intercepted electronic message according to the recipient's public key. Further, Richard does not claim or disclose the ability to encrypt an intercepted electronic message using the recipient's public key which is retrieved by the first set of computer readable instructions from a second computer readable medium or upstream server. Richard does not claim or disclose any computer readable instructions which can intercept and encrypt an electronic message.

In the present invention, Public Keys can be stored in a plurality of locations thereby providing for a decentralized storage system. This decentralized key lookup improves lookup performance, reduce storage needs for any one server, and increases fault tolerance for the decentralized storage system. Richard, however, does not manage Public Keys, but uses Public Keys in its operation. Specifically, Richard is limited to a system that looks to other directory servers to see if Public Keys are available to the directory server. (Richard, col 9, lines 5461). Richard performs no interception or encryption of electronic messages.

Further, if the certificate issuer is not known, Richard specifically states that "the directory acts as a directory client to attempt to find a known certificate issuer." (Richard, col 9, lines 63-65). Therefore, Richard is not directed to the decentralized management of public keys for encryption, but only for verification of client identify. (Richard, col 7, lines 56-65).

Richard is directed to a system that is used to determine access rights based upon the message senders identify. (Richard, col 2, lines 18-22). In Richard, the goal is to insure secured communications based upon the identity of the sender and client. (Richard, col 3, lines 18-22). Richard does not claim or disclose that there are Public

Keys established in a plurality of computer readable mediums so that decentralized storage of Public Keys is performed for encryption. Richard seeks to allow or limit access to information based upon the client's identify which associated with a Distinguishing Name. Specifically, Richard states that, "A client must have a verifiable identity in order for secure communications to continue." (Richard, Abstract, 3d sentence). Further, Richard state that, "a response may be obtained from a directory server which indicates whether the client has enough privileged to get the requested information...." (Richard, col 6, lines 64-67). In the present invention, secured communications is not necessary since the present invention is directed to the management of decentralized storage and publication of Public Keys.

The invention of Richard must have a "client must have a verifiable identify in order for secured communications to continue." (Richard, Abstract, 3d sentence). In the present invention, it is not necessary for the client to have "verifiable identify" since the present invention is directed to the decentralized storage and publication of Public Keys. The present invention supports secured communications by providing efficient and decentralized storage of Public Keys. However, the present invention does not require the identify of the client to be verifiable since Public keys are just that, public.

Richard further teaches away from decentralized storage since it is specifically directed to allowing the client and the server to be located on the same machine. (Richard, col 2, lines 57-59). By specifically, allowing the invention of Richard to function on a single computer, Richard clearly teaches away from a decentralized storage system for Public Key. Further, Richard specially, states that it can "act as a stand-alone server ...." (Richard, col 3, lines 15-17). By being able to act as a stand

alone server, again, Richard teaches away from a decentralized storage system for Public Keys. Richard uses direct access for client information as Richard states that the "server determines via the direct access component, what type of access the client is entitled to have." (Richard, col 7, lines 2-4).

As for the reference to Public Keys in Richard, Richard does not have decentralized management of Public Keys. Rather, Richard is concerning with the integrity and privacy of the "Public Key certificates, certificate revocation lists, pending certificate requests, Certificate Authority Policy, and other information" stored on the directory server. (Richard, col 3, lines 41-48). Richard is used to grant or deny access to this information, **not** to manage the information stored on the directory server. Richard does not claim or disclose the decentralized management of Public Key certificates, but only the ability to allow or restrict access to Public Key certificates located on a directory server. (Richard, col 3, lines 41-48). There is no disclosure in Richard that is directed to the decentralized management and retrieval of Public Keys.

If the Public Key of the client is unknown to the server of Richard, Richard in unable to determine the validity of the client certificate without knowledge of the certificate issuer. Again, this teaches away from the management decentralized Public Keys since Richard relies upon a Public Key system in order to match a internally stored public key for comparison and verification. (Richard, Fig 6A, 86). Richard is not directd to decentralized storage as further evidenced by block 86 of Figure 6A. Block 86 specificallly states that "The directory service verifies that the digital signature matches the internally stored public key of the certificate issuer." (Fig. 6A, 86). Since Richard states that the Public Key is an "internally stored public key", Richard does not claim or

disclose decentralized storage of Public Keys. In fact, claim 24 of Richard includes a database for specifically storing a public key. (Richard, Claim 24). Richard even contains one embodiment where the "digital signature on the issuer's certificate **matches the internally stored public key of the certificate issuer**." (Richard, col 10, lines 29-31) (emphasis added). Further, the invention of Richard relies upon the directory service have an "internally stored public key of the certificate issuer" and therefore is not directed to the management of decentralized keys. (Richard, Fig 6A, 86). Richard simply uses Public Keys and does not maintain decentralized storage and publication of Public Keys as in the present invention.

The present invention uses the root and secondary server to store the public keys in a plurality of locations. This structure allows for an encryption system using a decentralized storage and publication system for Public Keys. However, Richard specifically teaches away from the structure. Specifically, Richard states, "The present invention utilizes secure distributed directory services to maintain a public key infrastructure, and **does not operate in the conventional global, top-down hierarchy** using a 'meta-certifier', who must certify all users in order to provide the desired level of security." (Richard, col 2, lines 4-9) (emphasis added). Therefore, Richard does not contemplate decentralized storage or Public Keys, but states that "a particular message sender is identified in a given distributed directory service, using designated policy statements, permits the message recipient to determine degree of trust to be given to a message sender." (Richard col 2, lines 19-22). The present invention is not concerned with trust for the sender, but rather the management of the Public Key for encryption.

Respectfully, Richard does not anticipate the independent claims, as amended and the associated dependent claims in the present invention.

CONCLUSION

Richard is limited to having to have already stored the public key to verify the user. Richard, therefore, needs to have discovered the public key before it is operational. However, the present invention is a method for discovering Public Keys for use with encryption. The present invention does not need to have the Public Keys locally available as it is a system and method for discovering Public Keys.

Respectfully, the Applicant requests that the independent claims, as amended, and associated dependent claims, be allowed to pass to issuance in the normal course of Patent Office business.

Respectfully submitted,

Douglas W. Kim
Registration No. 44,828
McNair Law Firm, P.A.
P.O. Box 10827
Greenville, SC 29603-0827
Telephone: (864) 232-4261
E-mail: dkim@mcnair.net
Attorney for the Applicant